UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,137	08/11/2000	Michel Maillard	11345.023001	8272

22511 7590 12/28/2004

OSHA & MAY L.L.P.
1221 MCKINNEY STREET
HOUSTON, TX 77010

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 12/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/622,137	MAILLARD ET AL.	
	Examin r	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on th cover sh et with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,4-20 and 30-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,4-20 and 30-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. Claims 2, 4-20, and 30-35 are pending in this office action, claims 34 and 35 newly added.

2. Applicant's arguments, filed November 19, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claim 2, 4-10, 12, 14-18, and 30-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Tsuria (U.S. Patent No. 6,178,242).

Regarding claim 30, Tsuria teaches a method of recording transmitted digital data, comprising:

- Encrypting transmitted digital information of the transmitted digital data by a recording encryption key (fig. 2, ref. num 145);
- Storing the encrypted, transmitted digital information by a recording means on a recording support medium (fig. 2, ref. num 145);

- Encrypting an equivalent of the recording encryption key by a recording transport key (fig. 2, ref. num 175); and
- Storing the equivalent of the recording encryption key to the support medium together with the encryption information (fig. 2, ref. num 175),
    - Wherein at least one of the encryption key and recording transport key is stored on a portable security module associated with the recording means (col. 8, lines 52-59).

Regarding claim 31, Tsuria teaches a system for recording transmitted digital data, **wherein the transmitted digital data** is encrypted by a recording encryption key, comprising:

- A receiver/decoder for at least receiving the encrypted, transmitted digital data (fig. 1, ref. num 110); and
- A recording means for recording the encrypted, transmitted digital data to a recording support medium, along with an equivalent of the recording encryption key (fig. 1, ref. num 130),
    - Wherein the equivalent recording encryption key is encrypted via a recording transport key and stored with the recording means (fig. 2, ref. num 175).

Regarding claim 34, Tsuria teaches a system for recording transmitted digital data, wherein the transmitted digital data is encrypted by a recording encryption key, comprising:

- A recording support medium configured to store the encrypted transmitted digital data and an equivalent of the recording encryption key, wherein the equivalent of the recording encryption key is encrypted using a recording transport key (fig. 2, ref. num 175); and
- A portable security module configured to store at least one of the recording encryption key and the recording transport key (col. 8, lines 52-59).

Regarding claim 35, Tsuria teaches a recording support medium, comprising:

- Transmitted digital data, wherein the transmitted digital data is encrypted using a recording encryption key (fig. 2, ref. num 145); and
- An equivalent of the recording encryption key, wherein the recording encryption key is encrypted using a recording transport key (fig. 2, ref. num 175).

Regarding claim 2, Tsuria teaches the information encrypted by the recording encryption key (E (NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium (column 6, line 65 to column 7, line 1).

Regarding claim 4, Tsuria teaches the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means (column 6, lines 57-62).

Regarding claim 5, Tsuria teaches the decoder is associated with a portable security module used to store transmission access control keys (KO (NS), KO' (Op1, NS) etc.) used to decrypt the transmitted encrypted information (column 7, lines 48-56).

Regarding claim 6, Tsuria teaches:

- At least one of the recording encryption key (E (NE)) and/or recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) (column 7, lines 58-64) and
- The transmission access control keys (KO (NS), KO' (Op1, NS) etc.) function in accordance with a second encryption algorithm (CA) (column 8, lines 24-28).

Regarding claim 7, Tsuria teaches the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means (figure 2, reference number 145 transmitted to 175).

Regarding claim 8, Tsuria teaches the recording transport key (RT (A)) is encrypted by a further encryption key (KO (NSIM)) prior to being communicated to the recording means (figure 2, reference number ECM KEY).

Regarding claim 9, Tsuria teaches a central access control system communicates transmission access control keys (KO (NS), KO' (Op 1, NS) etc.) to the recording means (figure 1, reference number 110).

Regarding claim 10, Tsuria teaches the transmission access control keys (KO (NS), KO' (Op1, NS) etc.) are communicated to a portable security module associated with the recording means (figure 1, reference number 120).

Regarding claim 12, Tsuria teaches central access control system encrypts the broadcast access control keys (KO (NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means (figure 2, reference number TECM KEY).

Regarding claim 14, Tsuria teaches:

- Using a decoder means and associated security module and a recording means and associated security module (figure 1, reference numbers 110 and 120, and column 6, lines 63-65) and
- In which a copy of the recording transport key (RT (A)) is stored in at least one of the security module associated with the decoder means and/or the security module associated with the recording means (column 8, lines 52-59).

Regarding claim 15, Tsuria teaches the recording transport key (RT (A)) is generated by either the recording security modules or decoder security module and communicated to the other security module (figure 2).

Regarding claim 16, Tsuria teaches the recording transport key (RT (A)) is encrypted before communication to the other security module and decrypted by a key unique (KO (NS)) to that other security module (column 8, lines 17-28).

Regarding claim 17, Tsuria teaches the decoder security module and recording security module (52) carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization (column 8, lines 17-28).

Regarding claim 18, Tsuria teaches the mutual authorization step is carried out using, inter alia, an audience key KI (C) known to both security modules (30,52) (column 8, lines 17-28).

Regarding claim 32, Tsuria teaches further comprising a decoder means and associated security module adapted to store a copy of the recording transport key (RT(A)) (fig. 1, ref. nums 110 and 120).

Regarding claim 33, Tsuria teaches in which the security module associated with the decoder means is adapted to descramble transmitted information using one of more transmission access keys prior to re-encryption by a session key for subsequent communication to the recording means (fig. 3, and col. 9, lines 57-65).

Claim Rejections - 35 USC § 103

5. Claims 11, 13, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (USPN '242) in view of Park (European Patent No. 714,204).

Regarding claim 11, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

Park teaches the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium (see page 8, lines 20-22 of Park).

It would have been obvious to one of ordinary skill in that art, at the time the invention was made, to combine the recording means directly descrambles transmitted

information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium, as taught by Park, to the method of Tsuria. It would have been obvious for such modifications because the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium would properly restore the encrypted transmission keys to a clear state so that the key can be used to further encrypt the information in the recording means.

Regarding claim 13, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request of authentification by the recording means using a key (KO (NSIM)) unique to that recording means.

Park teaches the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request being authenticated by the recording means using a key (KO (NSIM)) unique to that recording means (see page 8, lines 40-45 of Park).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means, as taught by Park, to the method of Tsuria. It would have been obvious for such modifications because the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means would provide a secure way for the recording means to request keys as needed from the central access control system.

Regarding claim 19, Tsuria teaches all of the subject matter of claims 1 and 14, as discussed above. However, Tsuria does not disclose the decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

Park teaches:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form (page 8, lines 10-19) and

- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)) (page 8, lines 20-22).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key, as taught by Park, to the method of Tsuria. It would have been obvious for such modifications because the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form would allow the security module to properly decrypt the encrypted data for proper restoration of the signal.

A session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key would secure the clear signal again before transmission to the recording device, thus making the secure digital recording device more secure.

Regarding claim 20, the combination of Tsuria/Park teaches the session key (K3 (NSIM)) is generated by one of the decoder security module or recording means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by the other security module (see column 8, lines 17-28 of Tsuria).

Response to Arguments

6. Applicant amends claim 31, adds claims 34 and 35.

7. Applicant argues:

a. Tsuria fails to teach two levels of encryption, namely encrypting data with a key, storing the data, encrypting the key that encrypted the data, and storing that encrypted key (page 7, last paragraph through page 8, second paragraph).

b. Park, when combined with Tsuria, does not make up for the deficiency of two levels of encryption (page 8, last paragraph through page 9, first paragraph).

c. The dependent claims are allowable based on their dependency on the independent claims (page 8, third paragraph).

Regarding argument (a), examiner disagrees with applicant. The abstract of Tsuria shows that the scrambled digital data segment (SDDS) is scrambled according to the control word (CW). This satisfies the limitation of encrypting digital data with a key (CW) and storing the digital data on a medium. The next limitation of encrypting the encryption key (CW) and storing the encrypted encryption key (CW) on the medium is

shown in the abstract as well. It states the ECM contains coded information for generating the CW, which is encoded using an ECM key. This means the control word (CW) that was used for scrambling the digital data, is then encrypted by the ECM key. The ECM key and the scrambled digital data are both stored on the medium, as can be seen in figure 2. Accordingly, the independent claims stand as rejected because Tsuria does indeed teach the two level encryption as claimed in the instant application.

Regarding argument (b), examiner disagrees with applicant. Based on the argument set forth by the examiner for argument (a), there is no deficiency in Tsuria. Therefore, claims 11, 13, 19, and 20 stand as rejected.

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand as rejected.

Conclusion

8. Applicant's amendment necessitated the new grounds of rejection. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

E. Moise

EMMANUEL L. MOISE
PRIMARY EXAMINER